

IN THE CLAIMS:

This listing of claims will replace all prior versions, and listing, of claims in the application:

1. (Previously Presented) A data processing unit for executing an encrypted software program, the data processing unit comprising:
 - a processor for decrypting the encrypted software program and for executing the software program, the processor including an identifying number functioning as a serial number for identifying the data processing unit, the identifying number being accessible only by the processor; and
 - a memory unit, the memory unit storing the decryption procedure, the encrypted program being encrypted using at least a portion of the identifying number; wherein, when the processor is to execute the software program, the software program is decrypted using the decryption procedure along with the identifying number.
2. (Original) The data processing unit as recited in claim 1 wherein the encrypted software program is stored in the memory unit.
3. (Original) The data processing unit as recited in claim 1 further comprising an external memory unit, wherein the encrypted software program is stored in an external memory unit.
4. (Original) The data processing unit as recited in claim 1 wherein the identifying number is a serial number.
5. (Original) The data processing unit as recited in claim 1 wherein the identifying number is associated with a plurality of data processing units.

6. (Previously Amended) A method for protecting software programs, the method comprising:
 - providing a data processing unit with an identifying number functioning as a serial number for identifying the data processing unit, the identifying number being accessible only by the processing unit;
 - encrypting a software program external to the data processing unit using at least a portion of the identifying number; and
 - decrypting the encrypted software program prior to execution of the software program by the data processing unit using the identifying number and a decryption procedure stored in the processing unit.
7. (Cancelled)
8. (Previously Presented) The method as recited in claim 6 wherein the identifying number is a serial number for the data processing unit.
9. (Previously Presented) The method as recited in claim 6 wherein the encrypted software program is stored external to the data processing unit.
10. (Previously Presented) The method as recited in claim 6 wherein the encrypted program is stored in the data processing unit.
11. (Previously Amended) A data processing system, the system comprising:
 - a host data processing unit, the host processing unit encrypting a software program using at least a portion of an identifying number functioning as a serial number for identifying the data processing unit; and
 - a target data processing unit, the target data processing unit decrypting the software program[[s]] with a software procedure using a decryption key based on the identifying number.
12. (Previously Amended) The system as recited in claim 11 wherein the identifying number is a serial number for the target data processing unit.

13. (Previously Presented) The system as recited in claim 11 further comprising a memory unit external to the target data processing unit, the memory unit storing encrypted software programs.
14. (Previously Presented) The system as recited in claim 11 further comprising a memory unit in the target data processing unit, the memory unit storing encrypted software programs prior to decryption.
15. (Previously Presented) The system as recited in claim 11 wherein an encrypted program is decrypted as an entity or on the fly prior to execution of the software program by the target data processing unit.
16. (Cancelled)
17. (Cancelled)
18. (Previously Presented) The system as recited in claim 15 wherein decrypted portions of the software program are stored in a protected memory unit accessible to only the target data processing unit.
19. (Previously Amended) A method for protecting an execution of a software file, the method comprising:
 - providing a target processor with an identifying number, that functions as a serial number for identifying the data processing unit, accessible only to the target processor;
 - encrypting the software file using at least a portion of the identifying/serial number;
 - applying the encrypted software file to the target processor; and
 - decrypting the encrypted software file using a decryption procedure stored in the target processor and the identifying/serial number.
20. (Cancelled)
21. (Previously Amended) An apparatus for secure transfer of software files, the apparatus comprising:

a first processor, the first processor having a program for encrypting a software file using an identifying number functioning as a serial number for identifying the data processing unit; and

a second processor, the second processor having a decryption procedure for decrypting the software file using at least a portion of the identifying/serial number stored in the second processor, the stored identifying/serial number being accessible only to the second processor.

22. (Cancelled)

23. (Previously Presented) The apparatus as recited in claim 21 wherein the at least a portion of the identifying/serial number is accessed by the first processor based on an indicia of the second processor.

24. (Original) The apparatus as recited in claim 21 wherein an encrypted software file is stored in an unsecured storage unit.

25. (Previously Amended) The apparatus as recited in claim 24 wherein the encrypted software file is stored in the unsecured storage unit prior to decryption.